International Journal of Mathematics and
Computer Science, **4**(2009), no. 1, 53–64

Explicit constructions of arithmetic lattices in SL(n, R)

Erik R. Tou[1], **Lee Stemkoski**[2]

[1]Department of Mathematics
Carthage College
2001 Alford Park Dr.
Kenosha, WI 53140, USA

[2]Department of Mathematics
Adelphi University
111 Alumnae Hall
Garden City, NY 11514, USA

e-mail: etou@carthage.edu, stemkoski@adelphi.edu

Abstract

In this paper we construct examples of arithmetic lattices Γ in $\mathrm{SL}_n(\mathbb{R})$ in an explicit manner that has not previously appeared in the literature. We give number-theoretic criteria for compactness of the quotient space $\Gamma\backslash\mathrm{SL}_n(\mathbb{R})$ and describe some particularly nice properties of Γ for the case $n = 3$.

1 Introduction

The theory of arithmetic groups has its origins in the work of Borel and Harish-Chandra (see particularly [3]). Much subsequent work has been done in exploring the arithmetic groups as they pertain to Lie theory (especially with classical linear algebraic groups), including criteria for compactness (cf. [7]). However, this work has been done in an abstract fashion that does not permit easy calculation of matrices or an examination their properties. In the present work, we develop explicit constructions of groups Γ in the ambient space $\mathrm{SL}_n(\mathbb{R})$. While such groups have been constructed in a more abstract setting (see especially Borel [2], p. 253 ff.), our construction derives its form from a particular collection of abelian number fields, which is in

Key words and phrases: Lattice, Lie Group, Arithmetic lattice, Division algebra, Primitive root, Galois.
AMS (MOS) Subject Classifications: Primary 11F06, Secondary 22E40.
ISSN 1814-0424 © 2009, http://ijmcs.future-in-tech.net

turn derived from Gaussian periods. In this way, we enable a computational examination of the groups Γ associated to these number fields, as well as the matrices and eigenvalues that arise from such groups. Following the lead of Morris [6], we give a necessary and sufficient condition for a lattice Γ to have compact quotient in $\mathrm{SL}_n(\mathbb{R})$. Lastly, we discuss some special properties of these lattices particular to the case $n = 3$.

2 Arithmetic lattices

In general, a subgroup Γ of a Lie group G is said to be a *lattice* in G if

1. it is discrete as a topological space (i.e., it possesses no accumulation points), and

2. it is cofinite in G (i.e., the volume of $\Gamma\backslash G$ is finite).

If the quotient space $\Gamma\backslash G$ is also compact, we say that Γ is a *cocompact* lattice. In this section, we consider lattices $\Gamma \subseteq \mathrm{SL}_q(\mathbb{R})$ that are *arithmetic.* While the presentation of arithmetic lattices often varies, we will take the work of Platonov and Rapinchuk [8] as our starting point.[1]

Provisional Definition. *Let $G \subseteq GL_n(\mathbb{C})$ be an algebraic group defined over $\mathbb{Q}$ and define $G_{\mathbb{Z}} = G \cap GL_n(\mathbb{Z})$. A subgroup $\Gamma \subseteq G$ is* arithmetic *if it is commensurable with $G_{\mathbb{Z}}$; i.e., the intersection $\Gamma \cap G_{\mathbb{Z}}$ has finite index in both Γ and $G_{\mathbb{Z}}$.*

However, this definition fails to account for some lattices that we wish to consider as arithmetic. Thus, we extend the provisional definition in what follows. Let V be an n-dimensional complex vector space and suppose that $V_{\mathbb{Q}}$ is a rational subspace of V such that

1. $\dim_{\mathbb{Q}}(V_{\mathbb{Q}}) = \dim_{\mathbb{R}}(V)$, and

2. $V_{\mathbb{Q}}$ generates V as a real vector space.

Then let M be a $\mathbb{Z}$-submodule of $V_{\mathbb{Q}}$ generated by the basis $\mathcal{E} = \{e_1, e_2, \dots, e_n\}$; in other words, $M = \mathbb{Z}e_1 + \mathbb{Z}e_2 + \cdots + \mathbb{Z}e_n$. We now state a more complete definition for arithmetic lattices.

[1] The interested reader should also consult [3] and [9].

Definition 1. *Let V be a finite-dimensional, complex vector space with rational subspace $V_{\mathbb{Q}}$, as described above. Furthermore, let $G \subseteq GL(V)$ be a linear algebraic subgroup, and take $G_M = \{g \in G : gM = M\}$. A lattice $\Gamma \subseteq G$ is $V_{\mathbb{Q}}$-*arithmetic *(or simply* arithmetic*) in G if Γ is commensurable with G_M for some $\mathbb{Z}$-submodule $M \subseteq V_{\mathbb{Q}}$.*

Note that when $e_1, e_2, \ldots, e_n$ are the elementary vectors, $M = \mathbb{Z}^n$ and $G_M = G_{\mathbb{Z}}$. Thus, the general definition reduces to the provisional definition when the basis $\mathcal{E}$ is chosen in the simplest way.

3 Constructing arithmetic lattices

Let L be a Galois extension of $\mathbb{Q}$ of odd prime degree q, and let σ be a generator of $\mathrm{Gal}(L/\mathbb{Q})$. Given a positive integer p, define the set map $\varphi : L^q \to \mathrm{Mat}_{q\times q}(L)$ by

$$\varphi(x_1, x_2, \ldots, x_q) = \begin{bmatrix} x_1 & x_2 & x_3 & \cdots & x_q \\ p\sigma(x_q) & \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_{q-1}) \\ p\sigma^2(x_{q-1}) & p\sigma^2(x_q) & \sigma^2(x_1) & \cdots & \sigma^2(x_{q-2}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p\sigma^{q-1}(x_2) & p\sigma^{q-1}(x_3) & p\sigma^{q-1}(x_4) & \cdots & \sigma^{q-1}(x_1) \end{bmatrix}.$$

Note that a similar set map was used by Morris [6] for $q = 3$. Now define $\mathcal{A} = \varphi(L^q)$; it is straightforward to show that $\mathcal{A}$ is a $\mathbb{Q}$-algebra. Lastly, define $\Gamma = \varphi(\mathcal{O}_L^q) \cap \mathrm{SL}_q(\mathbb{R})$, where $\mathcal{O}_L$ denotes the ring of integers in L.

Theorem 1. *Γ is an $\mathcal{A}$-arithmetic lattice in $SL_q(\mathbb{R})$.*

Proof. Since Galois automorphisms take algebraic integers to algebraic integers, $\varphi(\mathcal{O}_L^q)$ is a subset of $\mathrm{Mat}_{q\times q}(\mathcal{O}_L)$. It follows that $\varphi(\mathcal{O}_L^q) = \mathcal{A} \cap \mathrm{Mat}_{q\times q}(\mathcal{O}_L)$. Since $\mathcal{A}$ and $\mathrm{Mat}_{q\times q}(\mathcal{O}_L)$ are rings, $\varphi(\mathcal{O}_L^q)$ is also a ring. Next, note that L is a real field since it is a Galois extension of odd degree. (If L contained a nonreal number, complex conjugation would be a nontrivial automorphism of L and the Galois group would have even order.) Thus $\mathcal{A}$ and $\varphi(\mathcal{O}_L^q)$ are subrings of $\mathrm{Mat}_{q\times q}(\mathbb{R})$. Now make the following denotations:

1. $V = \mathrm{Mat}_{q\times q}(\mathbb{C})$, a q^2-dimensional complex vector space;

2. $V_{\mathbb{Q}} = \mathcal{A} = \varphi(L^q)$, a q^2-dimensional rational subspace of V;

3. $M = \varphi(\mathcal{O}_L^q)$, a subring of $V_{\mathbb{Q}}$;
4. $G = \mathrm{SL}_q(\mathbb{R})$, a subgroup of $GL(V)$.

From the general fact $L = \mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Q}$, it follows that M is a $\mathbb{Z}$-submodule of $V_{\mathbb{Q}}$. Next, we show that $\Gamma = G_M$. Suppose that $\gamma \in \Gamma$. Then, γ is an invertible element of the ring M. Thus, $\gamma M = M$ and so $\Gamma \subseteq G_M$. Conversely, consider an element $g \in G_M$. Since M contains the identity matrix $I = \varphi(1, 0, 0)$, we know from the definition of G_M that $g = gI \in M$. Since g is a determinant one matrix, $g \in \Gamma$ and so $G_M \subseteq \Gamma$. Thus, $\Gamma = G_M$ is an $\mathcal{A}$-arithmetic lattice in $\mathrm{SL}_3(\mathbb{R})$. □

4 The structure of the algebra

Since the algebra $\mathcal{A}$ is somewhat unwieldy, it is convenient to construct an alternative algebra that is more amenable to analysis. Then, we show that these two algebras are in fact isomorphic. This leads to precise criteria for $\mathcal{A}$ to be a division algebra, which enables us to determine conditions under which Γ is cocompact in $\mathrm{SL}_q(\mathbb{R})$.

Let L be a Galois extension over $\mathbb{Q}$ of odd prime degree q. Then the group $\mathrm{Gal}(L/\mathbb{Q})$ is cyclic; let σ be a generator of this group. Let p be a rational prime for which $x^q - p$ is irreducible over L. Using L, σ, and p, we can define an algebra $\tilde{\mathcal{A}}$ by

$$\tilde{\mathcal{A}} = \tilde{\mathcal{A}}_{L,\sigma,p} = \left\{ a_0 + a_1 z + \cdots + a_{q-1} z^{q-1} \ : \ a_i \in L \right\}$$

where multiplication resembles that of polynomials with the exception that multiplication involving the symbol z is not commutative. Specifically, we define $z \cdot a = \sigma(a) \cdot z$ for $a \in L$ and $z^q = p$. Reiner has shown that $\tilde{\mathcal{A}}$ is a central simple algebra over $\mathbb{Q}$ ([10], Theorem 29.6). We will show that $\mathcal{A}$ and $\tilde{\mathcal{A}}$ are isomorphic as $\mathbb{Q}$-algebras.

First, note that any matrix $A = \varphi(x_1, \ldots, x_q) \in \mathcal{A}$ is characterized by the fact that any entry $A_{i,j}$ of A satisfies

$$A_{i,j} = \pi(i,j) \cdot \sigma^{i-1}(A_{1,\tau(j)}), \tag{4.1}$$

where

$$\pi(i,j) = \begin{cases} 1 & \text{if } i \leq j \\ p & \text{if } i > j \end{cases}$$

and $\tau(j) = \tau_i(j) = [(j-i) \bmod q] + 1$ captures the cyclic permutation for each row of the matrix.

Theorem 2. *Let $\varphi : L^q \to Mat_{q\times q}(L)$ be defined as above, and $\mathcal{A} = \varphi(L^q)$. Then the map $\Phi : \tilde{\mathcal{A}} \to \mathcal{A}$ defined by*

$$\Phi(x_1 + x_2 z + \cdots + x_q z^{q-1}) \;=\; \varphi(x_1, x_2, \ldots, x_q)$$

is an isomorphism of $\mathbb{Q}$-algebras.

Proof. First, note that the map Φ is well-defined since every element of $\tilde{\mathcal{A}}$ may be written uniquely as a linear combination of powers of z with exponent less than q. Clearly, Φ is a bijective set map and is also an additive homomorphism. To verify that Φ is a ring homomorphism, we require a formula for multiplication in $\tilde{\mathcal{A}}$. To this end, let

$$(x_1 + x_2 z + \cdots + x_q z^{q-1}),\ (y_1 + y_2 z + \cdots + y_q z^{q-1}) \;\in\; \tilde{\mathcal{A}}\,.$$

Then,

$$\begin{aligned}
&(x_1 + x_2 z + \cdots + x_q z^{q-1})(y_1 + y_2 z + \cdots + y_q z^{q-1}) \\
&= \sum_{j=1}^{q} \left(\sum_{m=1}^{q} x_m \cdot z^{m-1} \cdot y_{\tau(j)} \cdot z^{\tau(j)-1} \right) \\
&= \sum_{j=1}^{q} \left(\sum_{m=1}^{q} x_m \cdot \sigma^{m-1}(y_{\tau(j)}) \cdot z^{\tau(j)-1+m-1} \right),
\end{aligned}$$

where $\tau = \tau_m$ is the permutation described earlier. Note that $\tau(j)-1 = j-m$ if $m \le j$ and $j-m+q$ if $m > j$. Consequently, $z^{\tau(j)-1+m-1} = \pi(m,j) z^{j-1}$ and we get

$$\sum_{j=1}^{q} \left(\sum_{m=1}^{q} \pi(m,j) \cdot x_m \cdot \sigma^{m-1}(y_{\tau(j)}) \right) z^{j-1}\,.$$

Now define the matrix W by

$$W \;=\; \Phi((x_1 + x_2 z + \cdots + x_q z^{q-1})(y_1 + y_2 z + \cdots + y_q z^{q-1})).$$

Clearly, the elements in the first row of W are the coefficients of the above polynomial expression in z. Specifically,

$$W_{1,j} = \sum_{m=1}^{q} \pi(m,j) \cdot x_m \cdot \sigma^{m-1}(y_{\tau(j)}).$$

Now consider the matrices

$$\begin{aligned} X &= \Phi(x_1 + x_2 z + x_3 z^2 + \cdots + x_q z^{q-1}) \\ Y &= \Phi(y_1 + y_2 z + y_3 z^2 + \cdots + y_q z^{q-1}) \end{aligned}$$

and let $Z = XY$. From the definition of matrix multiplication, we have

$$Z_{i,j} = \sum_{m=1}^{q} X_{i,m} \cdot Y_{m,j}.$$

By Equation 4.1, this means that

$$Z_{i,j} = \sum_{m=1}^{q} \pi(i,m) \cdot \pi(m,j) \cdot \sigma^{i-1}(X_{1,\tau_i(m)}) \cdot \sigma^{m-1}(Y_{1,\tau_m(j)}).$$

Thus, the entries in the first row of Z are

$$Z_{1,j} = \sum_{m=1}^{q} \pi(m,j) \cdot X_{1,m} \cdot \sigma^{m-1}(Y_{1,\tau_m(j)}).$$

Since the matrices W and Z are completely characterized by the entries $W_{1,j}$ and $Z_{1,j}$, and since $x_j = X_{1,j}$ and $y_j = Y_{1,j}$, it follows that $W = Z$. Thus,

$$\begin{aligned} &\Phi((x_1 + \cdots + x_q z^{q-1})(y_1 + \cdots + y_q z^{q-1})) \\ &= \Phi(x_1 + \cdots + x_q z^{q-1})\Phi(y_1 + \cdots + y_q z^{q-1}) \end{aligned}$$

and Φ is a ring homomorphism. Since Φ is also $\mathbb{Q}$-linear, it is a $\mathbb{Q}$-algebra isomorphism. □

As mentioned earlier, we are particularly interested in when $\mathcal{A} = \varphi(L^q)$ is a division algebra. Fortunately, such a criterion exists for $\tilde{\mathcal{A}}$.

Theorem 3. *The algebra $\tilde{\mathcal{A}}$ is a division algebra if and only if p is not the norm of an element in $L^\times$; i.e., $p \notin N_{L/\mathbb{Q}}(L^\times)$.*

Proof. This is proven by Reiner ([10], Theorem 30.4.iii). □

Since $\tilde{\mathcal{A}}$ is isomorphic to $\mathcal{A}$, Theorem 3 holds for $\mathcal{A}$. We supplement this result with an observation about eigenvalues of matrices in $\mathcal{A}$.

Proposition 1. *If* $\mathcal{A} = \varphi(L^q)$ *contains a nonscalar matrix with a rational eigenvalue, then* $\mathcal{A}$ *is not a division algebra.*

Proof. Let $X \in \mathcal{A}$ be a nonscalar matrix with nonzero eigenvalue $\lambda \in \mathbb{Q}$. Since matrices in $\mathcal{A}$ give linear transformations of the vector space L^q, there exists a nonzero $v \in L^q$ such that $X(v) = \lambda \cdot v$. Then the matrix $Y = X - \lambda \cdot I \in \mathcal{A}$ is nonzero (since X is not a scalar matrix), and by the existence of v it follows that Y is noninvertible. Therefore, $\mathcal{A}$ is not a division algebra. □

5 Identifying cocompact lattices

We now consider the matter of cocompactness. Fortunately, there exists an elegant criterion to determine whether an $\mathcal{A}$-arithmetic lattice Γ is cocompact.

Theorem 4 (Godement compactness criterion). *Let* G *be a semisimple algebraic group defined over* $\mathbb{Q}$*. The quotient space* $G_{\mathbb{Z}}\backslash G$ *is compact if and only if* $G_{\mathbb{Z}}$ *contains no nontrivial unipotent elements.*

Proof. This appears in several places; cf. Mostow and Tamagawa [7]. □

For the present work, we wish to make use of a modified version of this theorem.

Theorem 5. *Let* Γ*,* $\mathcal{A}$*, and* G *be defined as in Theorem 1. The following are equivalent:*

1. *the quotient space* $\Gamma\backslash G$ *is compact,*

2. Γ *has no nontrivial unipotent elements,*

3. $\mathcal{A}$ *has no nontrivial unipotent elements.*

Proof. By definition, Γ is commensurable with $G_{\mathbb{Z}}$. Thus, $\Gamma\backslash G$ is compact if and only if $G_{\mathbb{Z}}\backslash G$ is compact (cf. [9], p. 170). Next, we show that Γ has nontrivial unipotent elements precisely when $G_{\mathbb{Z}}$ has nontrivial unipotent elements. A unipotent matrix u satisfies $(u - I)^n = 0$ for some $n \in \mathbb{Z}^+$. Any positive integer power of u is also unipotent, since $(u^m - I)^n = (u - I)^n(u^m + u^{m-1} + \cdots + 1)^n = 0$. Suppose $u \in G_{\mathbb{Z}}$ is unipotent. If Γ and $G_{\mathbb{Z}}$ are commensurable then the set $G_{\mathbb{Z}}/(\Gamma \cap G_{\mathbb{Z}})$ has finite order, and so the coset $u^r(\Gamma \cap G_{\mathbb{Z}})$ equals the identity coset $(\Gamma \cap G_{\mathbb{Z}})$ for some $r \in \mathbb{Z}^+$. Thus, $u^r \in \Gamma \cap G_{\mathbb{Z}}$ and is therefore a unipotent element in Γ. A similar argument will provide the converse.

Next, we observe that Γ contains nontrivial unipotent elements precisely when the algebra $\mathcal{A}$ contains nontrivial unipotent elements. One implication is trivial, as Γ is contained in $\mathcal{A}$. The other implication follows from [9] (cf. Theorem 10.18); for any unipotent element $u \in \mathcal{A}$ there exists $r \in \mathbb{Z}^+$ such that $u^r \in \Gamma$. □

We now bring together the above criteria in order to give a number-theoretic criterion for cocompactness.

Theorem 6. *Let Γ be an $\mathcal{A}$-arithmetic lattice in $SL_q(\mathbb{R})$, where $\mathcal{A}$ is derived from a Galois field L and a positive integer p, as described in Theorem 1. Then Γ is cocompact if and only if $p \notin N_{L/\mathbb{Q}}(L^\times)$.*

Proof. ($\Leftarrow$). Suppose that $p \notin N_{L/\mathbb{Q}}(L^\times)$. By Theorem 3, $\mathcal{A}$ is a division algebra. If Γ were not cocompact, then it would contain a nontrivial unipotent element u, by Theorem 5. Since all eigenvalues of u are equal to 1, Proposition 1 dictates that $\mathcal{A}$ *cannot* be a division algebra, a contradiction. Therefore Γ must be cocompact.

($\Rightarrow$). Suppose that Γ is cocompact but $p \in N_{L/\mathbb{Q}}(L^\times)$. By Theorem 3 $\mathcal{A}$ is not a division algebra. Since q is prime, Wedderburn's theorem (cf. [5], p. 171) implies that $\mathcal{A} \cong \mathrm{Mat}_{q\times q}(\mathbb{Q})$. From this we see that $\mathcal{A}$ contains unipotent elements. This contradicts the assumption that Γ is not cocompact, via Theorem 5. □

6 Examples and Properties

At this point, we have seen that any Galois field L of odd prime degree q will admit the construction of an arithmetic lattice in $\mathrm{SL}_q(\mathbb{R})$. Since every abelian number field is a subfield of $\mathbb{Q}(\zeta_n)$ for some primitive n^{th} root of unity ζ_n, we may explicitly construct all cubic Galois fields as subfields of these cyclotomic fields. To do this, let $n \in \mathbb{Z}^+$ be such that 3 divides $\phi(n)$, where ϕ is Euler's totient function. Then consider the cyclotomic field $K = \mathbb{Q}(\zeta_n)$. Since the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$ and has order $\phi(n)$, we know that it has a subgroup of index 3 and therefore K has a subfield L of degree 3 over $\mathbb{Q}$. Since $(\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, the cubic field L is also Galois.

We now determine L explicitly using Gaussian periods (cf. [4], [6]). Let H be a subgroup of index 3 in the Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$. Then define the Gaussian period $\omega = \sum_{k\in H} \zeta_n^k = \sum_{k\in H} \cos(\frac{2\pi k}{n}) \in \mathbb{R}$. Since ω is real, it follows that $L = \mathbb{Q}(\omega)$ is a real field. By Theorem 1, we may combine L with a prime p to construct a lattice Γ in $\mathrm{SL}_3(\mathbb{R})$.

Lemma 1. *Let p, q be distinct primes, and suppose that the q^{th} cyclotomic polynomial $f(x) = x^{q-1} + x^{q-2} + \cdots + x + 1$ is reducible modulo p. Then, p is not a primitive root modulo q.*

Proof. Suppose $f(x)$ is reducible modulo p, and let $g(x)$ be an irreducible factor of $f(x)$ with $\deg g(x) = r < \deg f(x) = q-1$. Since g is irreducible, the finite field $\mathbb{F}_{p^r}$ is isomorphic to $\mathbb{F}_p[\alpha]$ where α is a root of g. Since $\alpha^q - 1 = 0$ and q is prime, it follows that the order of α (as an element of $\mathbb{F}_{p^r}^\times$) is equal to q. By Lagrange's theorem q must divide $p^r - 1$; consequently, $p^r \equiv 1 \pmod q$. Since $r < q - 1$, it follows that p is not a primitive root modulo q. □

Theorem 7. *Let n, p be distinct primes with $n \equiv 1 \pmod 3$. Let H be an index 3 subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ and define the Gaussian period $\omega = \sum_{k\in H} \zeta_n^k$, where $\zeta_n = e^{2\pi i/n}$. Lastly, define $L = \mathbb{Q}(\omega)$. If p is a primitive root modulo n, then the lattice $\Gamma = \Gamma_{L,p}$ is cocompact in $SL_3(\mathbb{R})$.*

Proof. First of all, since $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ with order $\phi(n) = n - 1$ and $n \equiv 1 \pmod 3$, it follows that there exists a subgroup of index 3 in the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. We have already denoted such a subgroup by H.

Next, we know from Theorem 6 that $\Gamma_{L,p}$ will be cocompact precisely when $p \notin N_{L/\mathbb{Q}}(L^\times)$. To this end, let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ be nontrivial and suppose that $p = N_{L/\mathbb{Q}}(t) = t\sigma(t)\sigma^2(t)$ for some $t \in L^\times$. Since t and its Galois conjugates are contained in L, there is a positive integer m such that $pm = s\sigma(s)\sigma^2(s)$, where $s = a + b\omega + c\omega^2$ with $a, b, c \in \mathbb{Z}$ and $p \nmid \gcd(a, b, c)$. This means that $s\sigma(s)\sigma^2(s) = 0$ as an element of $(\mathbb{Z}/p\mathbb{Z})[\zeta_n]$. Since $(\mathbb{Z}/p\mathbb{Z})[\zeta_n] \cong (\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$ via the identification $\zeta_n \leftrightarrow x$, we have the following polynomial equation:

$$s_1(x)s_2(x)s_3(x) \ = \ 0 \ \in \ (\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle,$$

where $f(x)$ is the n^{th} cyclotomic polynomial and the polynomials s_1, s_2, s_3 are obtained from s, $\sigma(s)$, $\sigma^2(s)$, respectively. This shows the existence of zero divisors in $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x)\rangle$, so it is not an integral domain. Thus, $f(x)$ must be reducible modulo p. But this contradicts Lemma 1, since we assumed that p is a primitive root of the prime n. Therefore, $p \notin N_{L/\mathbb{Q}}(L^{\times})$. By Theorem 6, Γ is a cocompact lattice in $\mathrm{SL}_3(\mathbb{R})$. □

Since Theorem 7 requires that n be prime, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is cyclic and therefore has a unique subgroup of each possible order. This means that there is only one possible choice for the subgroup H; namely,

$$H = \{1 \leq j < n \mid \gcd(j,n) = 1,\ j^{(n-1)/3} \equiv 1 \pmod{n}\}.$$

This gives rise to a very simple method for generating cocompact lattices in $\mathrm{SL}_n(\mathbb{R})$.

Example 1. Select $n = 7$, with $\zeta_7 = \zeta$. Then, $H = \{1, 6\}$, $\omega = \zeta + \zeta^6$ and $L = \mathbb{Q}(\omega)$. Furthermore, the minimal polynomial of ω over $\mathbb{Q}$ is $\mu(x) = x^3 + x^2 - 2x - 1$ and L is Galois, so L is the splitting field of $\mu(x)$ over $\mathbb{Q}$. Since 3 and 5 are the primitive roots modulo 7, any prime $p \equiv 3, 5 \pmod 7$ will produce a cocompact lattice in $\mathrm{SL}_3(\mathbb{R})$.

Example 2. Select $n = 13$, with $\zeta_{13} = \zeta$. Then $H = \{1, 5, 8, 12\}$, $\omega = \zeta + \zeta^5 + \zeta^8 + \zeta^{12}$ and $L = \mathbb{Q}(\omega)$. Furthermore, the minimal polynomial of ω over $\mathbb{Q}$ is $\mu(x) = x^3 + x^2 - 4x + 1$ and L is Galois, so L is the splitting field of $\mu(x)$ over $\mathbb{Q}$. Since 2, 6, 7, and 11 are the primitive roots modulo 13, any prime $p \equiv 2, 6, 7, 11 \pmod{13}$ will give a cocompact lattice in $\mathrm{SL}_3(\mathbb{R})$.

Finally, we consider the eigenvalues of matrices in the arithmetic lattices $\Gamma \subseteq \mathrm{SL}_3(\mathbb{R})$. Using the explicit construction in Theorem 1, it is a simple matter to check that an element $\gamma = \varphi(x_1, x_2, x_3) \in \Gamma$ has characteristic polynomial

$$c_\gamma(r) \ = \ r^3 - T(x_1)r^2 + \big(T(x_1\sigma(x_1)) - p \cdot T(x_2\sigma(x_3))\big)r - 1,$$

where $T = \mathrm{Tr}_{L/\mathbb{Q}}$ is the number-theoretic trace. Note in particular that $c_\gamma(r) \in \mathbb{Z}[r]$. When Γ is cocompact, Proposition 1 implies that each eigenvalue of γ is algebraic of degree 3 over $\mathbb{Q}$. We more fully characterize the set of eigenvalues with the following result.

Proposition 2. *Suppose that Γ is a cocompact, $\mathcal{A}$-arithmetic lattice in $SL_3(\mathbb{R})$. The characteristic polynomial of every nonscalar matrix Y in the division algebra $\mathcal{A}$ is separable and irreducible. In particular, its eigenvalues are distinct.*

Proof. Let $f \in \mathbb{Q}[x]$ be the (cubic) characteristic polynomial of $Y \in \mathcal{A}$. Since irreducible polynomials in $\mathbb{Q}[x]$ are also separable, we need only rule out the possibility that f is reducible over $\mathbb{Q}$. This is easily done: a cubic polynomial reducible over $\mathbb{Q}$ must have a rational root, meaning that Y has a rational eigenvalue, contradicting Proposition 1. □

References

[1] James Arthur, David Ellwood, Robert Kottwitz, eds., Harmonic Analysis, The Trace Formula, And Shimura Varieties, Amer. Math. Soc., 2005.

[2] Armand Borel, Linear Algebraic Groups, 2nd ed., Springer-Verlag, 1991.

[3] Armand Borel, Harish Chandra, Arithmetic subgroups of algebraic groups, Bull. Amer. Math. Soc., **67** (1961), 579–583.

[4] Richard Crandall, Carl Pomerance, Prime Numbers: A Computational Perspective, 2nd ed., Springer, 2005.

[5] Nathan Jacobson, Basic Algebra II, W. H. Freeman, 1985.

[6] David Witte Morris, Introduction to arithmetic groups, Preprint.

[7] G. D. Mostow, T. Tamagawa, On the compactness of arithmetically defined homogeneous spaces, Ann. of Math., **76** 3 (1962), 446-463.

[8] V. Platonov, A. Rapinchuk, Algebraic Groups and Number Theory, Academic Press, 1992.

[9] M. S. Raghunathan, Discrete subgroups of Lie groups, Springer-Verlag, 1972.

[10] Irving Reiner, Maximal orders, Academic Press Inc., London, 1975.

[11] Atle Selberg, Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series, J. Indian Math. Soc., **20** (1956), 47–87.

[12] Audrey A. Terras, Harmonic Analysis on Symmetric Spaces and Applications, Springer-Verlag, 1985.

[13] Dorothy Wallace, The Selberg trace formula for $\mathrm{SL}(3,\mathbb{Z})\backslash\mathrm{SL}(3,\mathbb{R})/\mathrm{SO}(3,\mathbb{R})$, Trans. Amer. Math. Soc., **345** 1 (1994),1–36.